



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/650,440	08/27/2003	Frederic G. Thiele	END920030068US1	7247

26502 7590 11/13/2006

IBM CORPORATION
IPLAW IQ0A/40-3
1701 NORTH STREET
ENDICOTT, NY 13760

EXAMINER

PERUNGA VOOR, VENKATANARAY

ART UNIT	PAPER NUMBER
2132	

DATE MAILED: 11/13/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No. 10/650,440	Applicant(s) THIELE ET AL.	
	Examiner Venkat Perungavoor	Art Unit 2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
 - If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
 - Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 27 August 2006.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-20 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-20 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413) |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | Paper No(s)/Mail Date. _____ |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08) | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| Paper No(s)/Mail Date <u>8/27/03</u> . | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

Claim Objections

1. Claim 12 is objected to because the word "fourth" is misspelled.

Claim Rejections - 35 USC § 101

2. 35 U.S.C. 101 reads as follows:

Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

3. Claims 1-12, 17-20 are rejected under 35 USC § 101 as they recite a software program per se which is non-statutory subject matter. See MPEP 2106, IV, B, 1(a). Although a computer readable medium is disclosed, there is no mention of the program instructions being embodied on it.

Claim Rejections - 35 USC § 102

4. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

5. Claims 1-2, 4-5, 13-15, 17-18 are rejected under 35 U.S.C. 102(e) as being anticipated by U.S. Patent Publication 2003/0145228 A1 to Suuronen et al. (hereinafter Suuronen).

6. Regarding Claim 1, 13, 18, Suuronen discloses the classifying of packets into types containing virus-free(includes broadcast and network administration) and possible infected type that is sent to the scanner for further search see Par. 0021; and additionally for searching the database for new or known viruses see Fig. 1. Suuronen discloses three types packets IP packets(includes broadcast and administration) that cannot contain viruses, virus alert that might contain viruses, and virus free packets that after virus scanned are free of viruses see Fig.1- item 20, 28. And further discloses the updating of databases-packet classification and virus scanner to see if the network exploit is an new or known exploit.
7. Regarding Claim 2, 7, 14, Suuronen discloses the firewall being used for scanning for via lotion of rules and determination of web traffic including webcrawlers and broadacast packets see Par. 0009 & Fig. 1. Suuronen discloses the dropping of packets from the Firewall(14) that do not comply with the rules, see Fig. 1. And packet being examined if the database can find it or otherwise considered new see Fig. 1 item 24.
8. Regarding Claim 4, 17, Suuronen discloses the blacklisting of packets so that known exploits can no longer have access to network's destination see Par. 0007.

9. Regarding Claim 5, 15, Suuronen discloses the gateway being used being several communication networks see Fig. 2-5, whereby the gateway is an computing device that is easily adaptable on an network and not a dedicated device.

10. Regarding Claim 12, Suuronen discloses the packets being alerted when the packet is not a broadcast or administration, known exploit see Fig. 1.

Claim Rejections - 35 USC § 103

11. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

- (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

12. Claims 3, 8-11, 18, 20 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S Patent Publication 2003/0145228 A1 to Suuronen et al.(hereinafter Suuronen) in view of U.S. Patent 6853619 to Grenot.

13. Regarding Claim 3, 18, Suuronen does not disclose the searching based on signature for known exploits. However, Grenot discloses the searching based on signature for known exploits see Col 6 Ln 8-25. It would be obvious to one having ordinary skill in the art at the time of the invention to include the signature

searching for known exploits in the invention of Suuronen in order to search based on a quantitative measure as taught in Col 8 Ln 48-52 of Grenot.

14. Regarding Claim 8, Suuronen does not disclose the examining of gateways and sub-net masks. However, Grenot discloses the examining of gateways and sub-net masks see Col 6 Ln 26-35. It would be obvious to one having ordinary skill in the art at the time of the invention to include the examining of gateways and sub-net masks in the invention of Suuronen in order to examining flows as taught in Grenot see Col 6 Ln 26-35.

15. Regarding Claim 9-11, 20, Suuronen does not disclose the comparing of IP addresses and protocols. However, Grenot discloses the comparing of IP addresses and protocols see Col 5 Ln 63-Col 6 Ln 3 & Col 3 Ln 13-23. It would be obvious to one having ordinary skill in the art at the time of the invention to include the in the comparing of IP addresses and protocols invention of Suuronen in order to have a first line of defense against an attack.

16. Claims 6, 16 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S Patent Publication 2003/0145228 A1 to Suuronen et al. (hereinafter Suuronen) in view of NPL to Stallings.

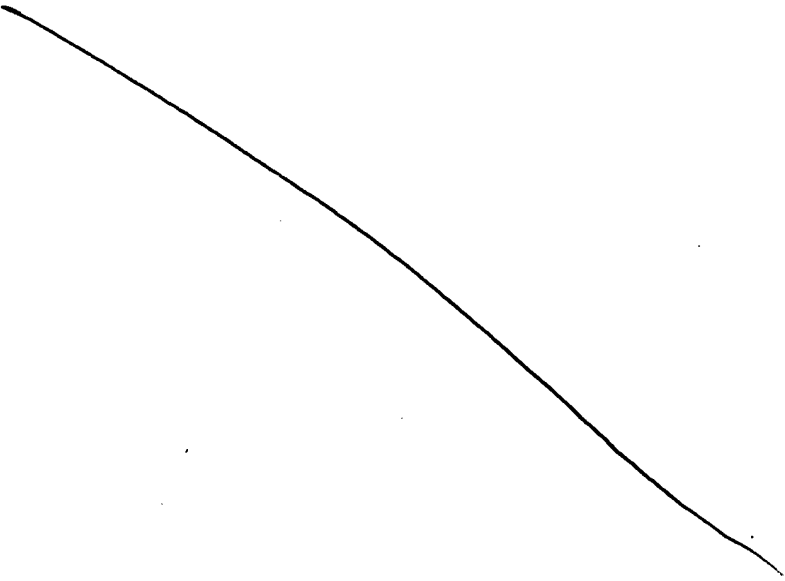
17. Regarding Claim 6, 16, Suuronen does not disclose the honeypots. However, Stallings discloses the honeypot see Page 580. It would be obvious to one having ordinary skill in the art at the time of the invention to include honeypots in the invention of Suuronen in order to divert the attacker as taught in Stallings see Page 580.

Conclusion

18. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

See Notice of Reference Cited

19. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Venkat Perungavoor whose telephone number is 571-272-7213. The examiner can normally be reached on 8-4:30. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

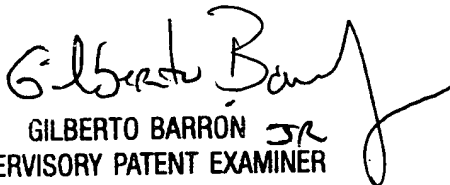


Art Unit: 2132

20. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Venkat Perungavoor
Examiner
Art Unit 2132

VP
11/7/2006


GILBERTO BARRON JR
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100